IDR Prüfungsleitlinie IDR-L 113-3 „Risiken ohne Prüfung der IT“

Stand: 09.2023

Autor_innen:

Tim Fritsch, Revisionsamt der Stadt Frankfurt a. Main

Sven Alsdorf, Gemeindeprüfungsanstalt Nordrhein-Westfalen

Nina Kramer, Rechnungsprüfungsamt Stadt Leverkusen

Roland Strauss, Rechnungsprüfungsamt Stadt Leipzig

Inhalt

I. Abbildungsverzeichnis

II. Dokumentenhistorie

Version	Datum	Verfasser	Änderung / Grund	Status
01.0	12.2021	T. Fritsch	Erstellung des Dokuments – Erste Stichpunkte	In Arbeit
01.0	01.2022	T. Fritsch	Erweiterung Themenbereich „ERSTE Prioritäten“	In Arbeit
01.0	03.2022	T. Fritsch	Erstellung Entwurf für AK DITS	In Arbeit
01.0	04.2022	T. Fritsch	Ausgestaltungen Prioritäten und Inhalt (ENTWURF für Tagung AK DITS)	In Arbeit
01.1	05.2022	T. Fritsch, R. Strauss, N. Kramer, S. Alsdorf	Gesamtaufbau	in Arbeit
01.1	06.2022	S. Alsdorf	Gesamtaufbau (Nacharbeiten aus dem Workshop Mainz)	in Arbeit
01.1	12.2022	T. Fritsch	Sichtung / Einpflegen von Änderungen	in Arbeit
01.1	01.2023	R. Strauss	Ergänzung „Allgemeiner Risiken bei fehlenden Prüfhandlungen“	In Arbeit
01.1	01.2023	AK DITS	Ergänzungen bei den Risiken	ENTWURF
01.1	09.2023	AK DITS	Einarbeitung redaktioneller Anmerkungen	FINAL

1. Vorbemerkungen[1]

IT ist in sämtlichen Bereichen der Kommunen vorhanden. Eine Nutzung und Einbindung gibt es vom Computer-Arbeitsplatz über vollständige eAkten bis hin zu speziellen Fachverfahren in allen Bereichen. Eine Buchhaltung ohne digitales Buchführungssystem ist undenkbar. Der Trend der Einbindung von elektronischen Prozessen und Abläufen wird sich im Zeitalter der „digitalen Revolution“ weiter verstärken. Grund hierfür sind u.a. auch die einzelnen Gesetzgebungen (eGovernment-Gesetz, eJustice-Gesetz, Onlinezugangsgesetz, EU-Datenschutzrichtlinie u.v.m.), welche insbesondere mit ihren Regelungen den öffentlichen Dienst betreffen. Die digitale Transformation der öffentlichen Verwaltungen wird darüber hinaus durch zahlreiche „Digitalisierungsoffensiven“ in einzelnen Bundesländern wirksam verstärkt.

Die zunehmende Nutzung von IT-Systemen bietet nicht nur zahlreiche Chancen, sondern birgt auch erhebliche Risiken. Mit dem ansteigenden Digitalisierungsgrad steigt auch die Abhängigkeit von technischen Systemen. Technische Störungen führen häufig im Zusammenhang mit einer unzureichenden Notfallabsicherung und fehlenden Redundanzen zu Behinderungen in den Arbeitsabläufen und damit zu einer Einschränkung in der Verwaltungstätigkeit. Neben persönlichen Haftungen und finanziellen Schäden besteht somit auch die Gefahr von Vertrauens- und Imageverlust in der Öffentlichkeit. Daneben können fehlerhaft konzipierte bzw. konfigurierte Elemente in der IT beispielsweise Unbefugten den Zugriff auf sensible Daten erleichtern. Durch solche Schwachstellen besteht die Möglichkeit, relevante Daten unbemerkt zu verändern oder bewusst zu manipulieren. Schlimmstenfalls stehen durch Sicherheitsvorfälle die für einen Prozess oder ein bestimmtes Produkt notwendigen kritischen IT-Anwendungen nicht zur Verfügung. Neben technischen Ursachen sorgen unter Umständen auch die Mitarbeitenden selbst im Umgang mit IT-Anwendungen durch fahrlässiges Verhalten oder ggf. sogar vorsätzlich falsches Handeln für eine Gefahr. Die »Awareness« für die Risiken bei Einsatz und Nutzung von IT und damit auch das Bewusstsein für die Notwendigkeit von IT-Prüfungen werden neben anderen unternehmensrelevanten Elementen zu einem der wichtigsten Handlungsfelder[2].

Dieses Dokument behandelt die Risiken, die mit einer unzureichenden oder sogar ausbleibenden örtlichen IT-Prüfung einhergehen.

[1] IDR-Eckpunktepapier der IT-Prüfung vom 28.06.2018

[2] Auszüge aus dem ISACA Leitfaden „Grundlagen der IT-Revision für den Einstieg in die Praxis“ Stand Juli 2016

2. Die IT als Prüfgegenstand und Prüfunterstützung

Innerhalb der Prüfung sind grundlegend zwei Themenblöcke zu unterscheiden, das **Prüfen der IT** (Infrastruktur, Prozesse, Software) und die Prüfungstätigkeit der modernen, zeitgemäßen Rechnungsprüfung mit und innerhalb von IT-Systemen sowie Fachverfahren, sprich **das Prüfen mit IT.**

Für die IT-Revision ergeben sich daraus die folgenden, relevanten Elemente, die entsprechend ihrer jeweiligen Inhalte ein gemeinsames oder ein aufeinander aufbauendes Prüfungsobjekt bilden.

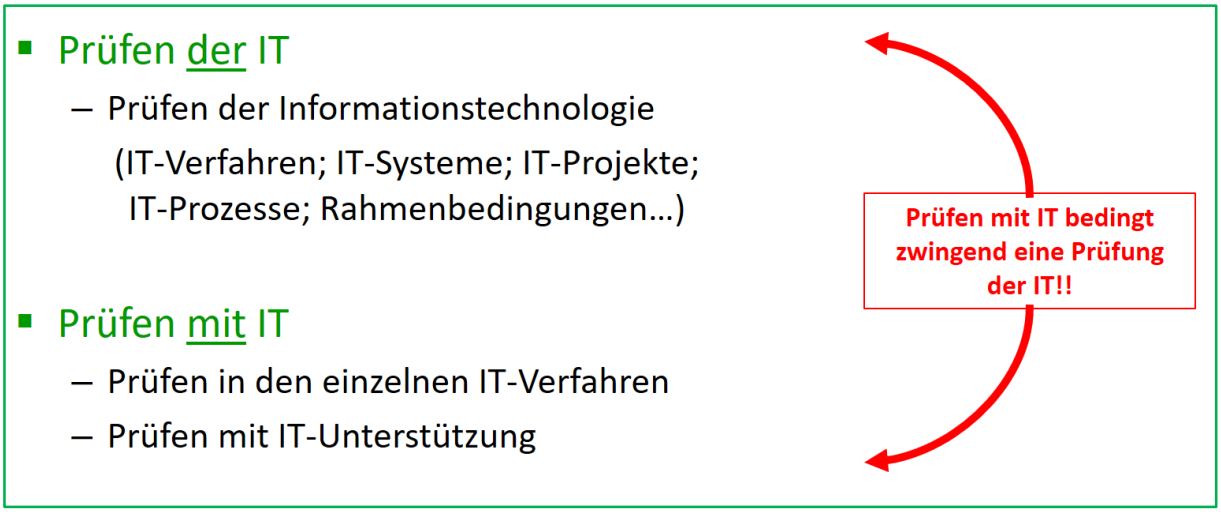

Abbildung 1- Prüfen mit IT / Prüfen der IT

Es wird deutlich, dass eine risikoorientierte Rechnungsprüfung einzig zielführend und abschließend sein kann, wenn beide Felder beachtet werden.

Eine Prüfung innerhalb eines nicht ordnungemäßen oder zweckgemäßen IT-Verfahrens, welches in einem nicht ordnungemäßen oder zweckgemäßen IT-Umfeld betrieben wird, kann Kontrolllücken und Manipulationsmöglichkeiten bieten, die mit einer reinen Inhaltprüfung nicht aufgedeckt werden können.

Zusätzlich können die wirtschaftlichen Faktoren nicht abschließend beurteilt werden. Ist der Einsatz angemessen? Im Folgenden stehen diejenigen Risiken im Fokus, die mit einer ausbleibenden Prüfung der IT einhergehen.

3. Risiken unzureichender IT-Prüfungshandlungen (Prüfen der IT)

- **Gesetzliche Pflichtaufgaben werden nicht erfüllt**
  Bei nicht vorhandener IT-Prüfung können die in den jeweiligen Landesgesetzen enthaltenen Vorgaben hinsichtlich der IT-Verfahrensprüfung und/oder der Programm- und Anwendungsprüfung nicht oder nur unzureichend erfüllt werden. Somit wird ggf. gesetzlich pflichtigen Aufgaben nicht nachgekommen. Gleichwohl ist zu berücksichtigen, dass sich die Notwendigkeit von Prüfhandlungen im Zusammenhang mit IT auch indirekt aus gesetzlichen Bestimmungen heraus ergeben können (z.B. Einhaltung der GOBD oder Wirksamkeit des IKS). In Bereichen ohne gesetzliche Grundlage zur Prüfpflicht ergeben sich ebenfalls folgende Risiken.

- **Die Integrität der geprüften Inhalte kann nicht sichergestellt werden**
  Werden Verwaltungsakte und Ergebnisse geprüft, welche aus den einzelnen IT-(Fach-)Verfahren resultieren, so ist ohne eine Prüfung der IT nicht sichergestellt, ob die Rahmenbedinungen (Berechtigungswesen / Unveränderbarkeit / Nachvollziehbarkeit etc.) korrekt sind und somit auch nicht, ob die vorliegenden und geprüften Inhaltsdaten stimmig sind. Eine vollständig progressive und retrogragrade Prüfung[3] ist ohne Prüfung der genutzten Werkzeuge (IT-(Fach-)Verfahren / IT-Infrastruktur), mit welchen die Inhalte erstellt wurden, nicht möglich.
  Dies birgt die Gefahr der Durchführung von ineffizienten bzw. unwirtschaftlichen Prüfungstätigkeiten.

- **Gefahr von ineffizientem bzw. unwirtschaftlichem Verwaltungshandeln**
  Ohne eine IT-Prüfung werden bestimmte Aufgaben der IT innerhalb der zu prüfenden Bereiche ggf. nicht ordnungsgemäß, zweckgemäß und wirtschaftlich durchgeführt. Dies führt zu finanziellen und rechtlichen Problematiken, welche wiederum in Imageschäden und Vertrauensverlusten hinsichtlich der Öffentlichkeit münden. Die örtliche IT-Prüfung kann wesentlich zu einem effizienteren und wirtschaftlicheren Verwaltungshandeln beitragen, wenn die nicht ordnungsgemäßen, nicht zweckmäßigen und unwirtschaftlichen Sachverhalte frühzeitig festgestellt und im Rahmen der Prüftätigkeiten an die Entscheidungsträger berichtet werden. Weiterhin sollte die (IT-)Prüfung den

[3] GoBD – 3.1 GRUNDSATZ DER NACHVOLLZIEHBARKEIT UND NACHPRÜFBARKEIT

geprüften Stellen - im Rahmen der Rolle als Berater und Innovator - präventiv eine Beurteilung der geplanten Maßnahmen und Strategien geben.

- **Erfüllung der Schutzziele und daraus resultierendes Risiko eines IT-Ausfalles**
  Grundsätzlich gilt für den Betrieb von IT-Systemen und IT-Infrastruktur der Schutz der darin enthaltenen Informationen. Die Erfüllung der Schutzziele richtet sich nach dem sogenannten Schutzbedarf. Eine fehlende Beurteilung und Prüfung der Schutzziele bzw. deren Nichteinhaltung kann erhebliche Auswirkungen und somit einen großen Schaden für die betroffenen Verwaltungen nach sich ziehen. Vor allem eine Prüfung derjenigen IT-Systeme zur Unterstützung finanzrelevanter und kritischer Geschäftsprozesse ist für das ordnungsgemäße Verwaltungshandeln unabdingbar (s. auch Tz. 4).

3.1. Allgemeine Risiken bei fehlenden Prüfhandlungen

Weiterhin bestehen grundsätzlich Risiken für Bereiche der Verwaltung, welche keiner Prüfung unterliegen. Diese Risiken sind natürlich auch für eine fehlende Prüfung der IT-Infrastruktur zu beachten:

- **Allgemeines Entdeckungsrisiko als Teil des Prüfungsrisikos**
  Das Entdeckungsrisiko besteht darin, dass im Rahmen von Prüfungshandlungen wesentliche Fehler des zu prüfenden Sachverhaltes nicht aufgedeckt werden (können). Im Ergebnis könnte – trotz wesentlicher Fehler – „Fehlerfreiheit“ bescheinigt werden. Mit der organisatorischen Einrichtung einer fachkundigen „IT-Prüfung“ wird eine wichtige Voraussetzung geschaffen, dass innerhalb angemessener Zeit ein sachgerechtes Prüfungsurteil gebildet werden kann.

- **Unzureichende Risikobewertung**
  Bei fehlender IT-Prüfung besteht die Gefahr, dass Risiken unterschätzt werden oder dass unwahrscheinliche Ereignisse, die jedoch katastrophale Auswirkungen haben können, unberücksichtigt bleiben.

- **Abwehrmaßnahmen werden nicht bzw. zu spät eingeleitet**
  Das Prüfen der IT (Infrastruktur, Prozesse, Software) ist kein Selbstzweck. Abweichungen bzw. Risiken sollen zeitnah festgestellt und kommuniziert werden, damit die geprüften Einrichtungen notwendige Korrekturmaßnahmen rechtzeitig ergreifen können.

- **Fehlende Präventivfunktion**
  Die Rechnungsprüfungsämter sind hinsichtlich der ihnen zugewiesenen Prüfungsaufgaben unabhängig und nicht an Weisungen gebunden. Sie entscheiden grundsätzlich nach eigenem Ermessen über Zeitpunkt, Gegenstand und Inhalt von Prüfungen. Es ist davon auszugehen, dass allein das „Vorhandensein“ von IT-Prüfern in der eigenen Organisationseinheit zu einer höheren Sorgfalt führt, da jederzeit mit gründlichen Prüfungen gerechnet werden muss.

- **Fehlende Beratungsfunktion der gemeindlichen Vertreter**
  Die Bürgermeister bzw. die Volksvertreter in den Kreistagen, den Stadt- und Gemeinderäten sind auf Zeit gewählt. Zur Erledigung ihrer Aufgaben sind sie auf die Unterstützung einer unabhängigen und sachkundigen Einrichtung angewiesen. Vor dem Hintergrund vielfältiger kommunaler Aufgaben und immer komplexer werdender IT-Verfahren und -systeme sind fachkundige Prüfungen und Stellungnahmen notwendig, die diese komplexen Fachgebiete für die Entscheider verständlich aufbereiten.

4. Schadenseintritte / Organisationsverschulden

Die Folgen nicht ordnungs- und zweckgemäß betriebener IT-Infrastrukturen und IT-(Fach-)Verfahren sind schwerwiegend. Hierzu zählen der Verlust der Informationssicherheit durch unbefugten Datenzugriff, Datenklau oder sogar Datenmanipulation (Integrität), die Durchführung unberechtigter Tätigkeiten (Zugriffe, Einsichtnahmen, dolose Handlungen) sowie Ausfallzeiten der einzelnen Soft- und Hardwarekomponenten. Die Ausfallzeiten führen wiederum zum Stillstand des Verwaltungshandelns für Beschäftigte sowie für die Bürger_innen. Hierdurch entsteht eine Gefährdungslage für die Öffentlichkeit durch massive Einschränkungen in den Verwaltungsabläufen (u. a. Transferleistungen aus den Bereichen Soziales und Jugend, Führerscheinstelle) und die Destabilisierung der kommunalen, digitalen Strukturen. Komplexe Probleme innerhalb der IT-Infrastruktur können mitunter zur Notwendigkeit des Ausrufs eines „Katastrophenfalls“ führen.[4]

Potenzielle Schadensfälle können beispielsweise eintreten durch:

- Manipulation der Infrastruktur

[4] s. Landkreis Anhalt Bitterfeld Juni 2021 – Katastrophenfall nach Hackerangriff

  - Hacking (Ransomware)
  - Datenklau
  - Gezielter Informationsdiebstahl
  - Interne Manipulation
  - Dolose Handlungen
  - …

- Ausfälle der Infrastruktur
  - Betrifft Teile der Verwaltung
  - Betrifft zentrale Zugänge
    - Internet
    - E-Mail
    - Fileserver
    - Telefon
    - ….
  - Betrifft IT-(Fach-)Verfahren

- Datenverlust
  - IT-(Fach-)Verfahren
  - Datenspeicher
  - E-Mail-Server

5. Fazit

Die Verwaltungsverantwortlichen müssen sich nachweislich mit potenziellen Schadenseintritten auseinandersetzen und unter Abwägung der Eintrittswahrscheinlichkeit sowie der möglichen Schadenshöhe geeignete, vorbeugende, organisatorische Maßnahmen treffen. Ziel ist es, das Risiko so weit wie möglich zu reduzieren und zu kontrollieren.

Die örtliche IT-Prüfung kann die Verwaltungsführung hierbei wesentlich unterstützen. Insofern könnte ein Verzicht darauf durchaus als organisatorisches Defizit verstanden werden, sofern nicht anderweitige Maßnahmen ergriffen werden.

Hierfür müssen in den örtlichen IT-Prüfungen die notwendigen finanziellen und personellen Ressourcen bereitgestellt werden. Insbesondere bei den personellen Ressourcen ist digitales Mindset und Skillset zur sachgerechten Prüfung und Beurteilung der oben genannten Risiken notwendig.